## REMARKS / DISCUSSION OF ISSUES

Claims 1-20 are pending in the application.

The Office action rejects claims 1-20 under 35 U.S.C. 101. The applicants respectfully traverse this rejection.

The Office action asserts that the claims are to "processes that do nothing more than solve mathematical problems [and/or] manipulate abstract ideas or concepts". The applicants respectfully disagree with this assertion.

The Office action references processes that convert one set of numbers into another set as unpatentable subject matter. The applicants respectfully note that such references are not relevant to the applicants claims, because each of the applicants' independent claims include the transmission of information from a first party to a second party, the processing of that information by the second party to generate other information, the transmission of the other information from the second party to the first party, and the processing of that other information by the first party. The applicants respectfully maintain that the transmission and processing of information constitutes patentable subject matter, and is not a mere conversion of one set of numbers into another set.

The Office action references claims to laws of nature, natural phenomenon, or abstract ideas. The applicants respectfully note, however, that exchanging and processing information to create a common secret/key for use by each party is neither a law of nature, a natural phenomenon, nor an abstract idea.

The Office action asserts that claim 19 is drawn to a computer program per se. The applicants respectfully disagree with this assertion, but in the interest of advancing prosecution in this case, claim 19 is amended to explicitly claim a computer readable media.

Because the applicants' claims are to new and useful processes and machines that do more than merely convert one set of numbers into another set, and do not, per se, claim a law of nature, a natural phenomenon, or an abstract idea, the applicants respectfully maintain that the rejection of claims 1-20 under 35 U.S.C. 101 should be withdrawn.

The Office action rejects claims 1, 9-12, and 16-19 under 35 U.S.C. 103(a) over Leighton et al. (USP 5,519,778, hereinafter Leighton) and Hoffstein et al. (USP 6,076,163). The applicants respectfully traverse this rejection.

Neither Leighton nor Hoffstein teaches or suggests calculating a common secret between two parties as a product of two symmetrical polynomials, as specifically claimed in each of the applicants' independent claims 1, 16, 17, and 19.

The Office action acknowledges that Leighton fails to provide this teaching, and asserts that Hoffstein teaches calculating a secret as a product of two symmetrical polynomials at column 3, lines 31-46 and FIG. 3. The applicants respectfully disagree with this assertion. At the cited text, Hoffstein teaches:

> "The above-described user identification technique can be converted to a digital signature technique by the prover applying a one-way hash function to $A_{g(x)}$ and a message m to generate a simulated challenge polynomial c(x) which may be used in conjunction with g(x) and f(x) to generate the response polynomial h(x). The verifier receives m, $A_{g(x)}$ and h(x), uses the one-way hash function to derive c(x), and compares $A_{h(x)}$ to $A_{g(x)}*(A_{f(x)}+A_{c(x)})$ in order to authenticate the digital signature of the prover. Alternatively, the signature might consist of c(x) and h(x). From this $A_{g(x)}$ can be recovered as $A_{h(x)}*(A_{f(x)}+A_{c(x)})$-1 and the hash of this quantity and the message m can be compared to the polynomial c(x). A desired security level in both the user identification and digital signature techniques may be provided by selecting appropriate constraints for the polynomials g(x), c(x) and h(x)." (Hoffstein, column 3, lines 31-46.)

As can be seen, the above text fails to identify a secret that is common to two parties, and the Office action fails to identify which of Hoffstein's terms are asserted to be a secret that is common to two parties. Additionally, the above text fails to identify any of Hoffstein's terms as being a symmetrical polynomial, and specifically does not identify any of the calculated terms as being a product of two symmetrical polynomials. The Office action fails to identify which of the terms in the above cited text is asserted to correspond to each of the applicants' claimed symmetrical polynomials, and fails to identify which of the above described operations corresponds to calculating a product of two such symmetrical polynomials.

In response to the applicants' prior remarks in this regard, the Office action refers to Hoffstein's FIG. 5, steps 1-4, and column 3, lines 45-65. The applicants acknowledge that steps 1-4 of Hoffstein's FIG. 5 teach the calculation of a polynomial h(x) as the product of two polynomials, g(x) and (f(x) + c(x)). However, the applicants respectfully note that nowhere in Hoffstein are the polynomials g(x) and (f(x) + c(x)) taught to be symmetrical polynomials, as expressly claimed in each of the applicants' independent claims.

The applicants also note that this product of two polynomials, h(x), is transmitted directly from Hoffstein's Prover to Hoffstein's Verifier. Because the product term h(x) is transmitted 'in the clear' for any and all other recipients to receive, it is obvious that this product term h(x) does not correspond to a 'secret' that is shared by two parties, as the term 'secret' is used in the art, and as the term 'secret' is used in the applicants' specification.

The Office action also fails to identify where either Leighton or Hoffstein teaches or suggests a first party that holds a symmetrical polynomial P(x,y) fixed in the first argument by a value $p_1$ and a symmetrical polynomial Q(x, z) fixed in the first argument by a value $q_1$, and sends the values $p_1$ and $q_1$ to a second party, as also specifically claimed in each of the applicants' independent claims. The Office action fails to identify which elements in either Leighton or Hoffstein corresponds to each of the claimed two symmetrical polynomials fixed in each of two values, fails to identify which elements in either Leighton or Hoffstein corresponds to each of two values at which each of such symmetrical polynomials are fixed, and fails to identify where either Leighton or Hoffstein teaches sending such values at which each of two symmetrical polynomials are fixed from one party to another.

MPEP 2142 states:

> "To establish a *prima facie* case of obviousness … the prior art reference (or references when combined) ***must teach or suggest all the claim limitations***… If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness."

Because the combination of Leighton and Hoffstein fails to teach or suggest each of the elements of each of the applicants' independent claims 1, 16, 17, and 19, upon which all of the other claims depend, and because the Office action fails to identify where either Leighton or Hoffstein teaches or suggests calculating a secret between two parties as the product of two symmetrical polynomials, the applicants respectfully maintain that the rejection of claims 1-20 under 35 U.S.C. 103(a) over Leighton and Hoffstein is unfounded, per MPEP 2142, and should be withdrawn.

In view of the foregoing, the applicants respectfully request that the Examiner withdraw the objection(s) and/or rejection(s) of record, allow all the pending claims, and find the application in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

/Robert M. McDermott/
Robert M. McDermott, Esq.
Reg. 41,508
804-493-0707

**Please direct all correspondence to:**
Corporate Counsel
U.S. PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001